

DOCKET NO: 198775US2

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

IN RE APPLICATION OF :  
TETSURO MOTOYAMA, ET AL. : EXAMINER: CHOUDHURY, A.  
SERIAL NO: 09/756,120 :  
FILED: JANUARY 9, 2001 : GROUP ART UNIT: 2145  
FOR: METHOD AND SYSTEM OF :  
REMOTE SUPPORT OF DEVICE USING  
EMAIL

APPEAL BRIEF

COMMISSIONER FOR PATENTS  
ALEXANDRIA, VIRGINIA 22313

SIR:

Applicants appeal the outstanding Final Rejection of June 20, 2007, finally rejecting each of pending Claims 1-12, 14-19, 21-28, 30, and 32-35.

I. REAL PARTY IN INTEREST

The above-noted application is assigned to Ricoh Company, Ltd., which is the real party in interest, having a place of business at Tokyo, Japan.

II. RELATED APPEALS AND INTERFERENCES

Applicant and Applicant's representative are not aware of any related appeals or interferences that will directly effect or be directly affected by or having a bearing on the Board's decision in the pending appeal.

### III. STATUS OF CLAIMS

Claims 1-12, 14-19, 21-28, 30, and 32-35 are pending in this application and the rejection of each of Claims 1-12, 14-19, 21-28, 30, and 32-35 is being appealed.

No claims were added, but Claims 13, 20, 29, and 31 were cancelled during prosecution of this application.

### IV. STATUS OF AMENDMENTS

A Request for Reconsideration was filed subsequent to the Final Rejection dated June 20, 2007. Accordingly, all previously filed Amendments have been considered by the Examiner and are reflected in the attached claims.

### V. SUMMARY OF CLAIMED SUBJECT MATTER

Claim 1 sets forth a computer-implemented remote device monitoring system.

In particular, Claim 1 recites a local monitoring computer configured (1) to collect information from a device connected to a first network using an SNMP protocol, and (2) to send the information to a remote monitoring computer connected to a second network via a wide area network using a protocol, which finds supports, e.g., in Figure 1, elements 105 (local monitoring computer); 108A (device); 106 (first network); 111 (remote monitoring computer); 114 (second network); and 110 (wide area network). See also page 7, lines 17-21 (SNMP); page 9, lines 6-10 (SNMP); and page 9, line 22 to page 10, line 7 (send to remote monitor).

Further, Claim 1 recites a remote monitoring computer configured to receive the information using the protocol and to store the information in association with an IP address of the device in a digital repository connected to the second network, which finds supports,

e.g., in Figure 1, element 111 (remote monitoring computer); 112 (digital repository); Figure 11 (IP address, information); page 11, lines 16-22; and page 19, lines 20-24).

Further, Claim 1 recites that the local monitoring computer is configured to automatically request the information from the device over the first network, without receiving any instructions from the remote monitoring computer requesting that the information be collected from the device, which finds supports, e.g., in Figure 4, steps S408 and S410; and page 15, lines 5-8.

Finally, Claim 1 recites that after initialization of the local monitoring computer, the local monitoring computer is configured to automatically send the information to the remote monitoring computer, without receiving any instructions from the remote monitoring computer requesting that the collected information be sent, which finds supports, e.g., in Figure 4, step S422; Figure 5, Figure 7; and page 15, lines 10-13.

Claim 16 is directed to a method for remotely monitoring network devices.

In particular, Claim 16 recites the step of collecting, by a local monitoring computer, information from a device connected to a first network using an SNMP protocol, which finds supports, e.g., in Figure 1, elements 105 (local monitoring computer); 108A (device); 106 (first network). See also page 7, lines 17-21 (SNMP); and page 9, lines 6-10 (SNMP).

Further, Claim 16 recites the step of sending, by the local monitoring computer, the information collected in the collecting step to a remote monitoring computer connected to a second network via a wide area network using a protocol, which finds supports, e.g., in Figure 1, elements 111 (remote monitoring computer); 114 (second network); and 110 (wide area network); and page 9, line 22 to page 10, line 7 (send to remote monitor).

Further, Claim 16 recites the step of receiving, by the remote monitoring computer, the information sent in the sending step, which finds supports, e.g., in Figure 8.

Further, Claim 16 recites the step of storing the information received in the receiving step in association with an IP address of the device in a digital repository connected to the second network, which finds supports, e.g., in Figure 9 and Figure 1, element 111 (remote monitoring computer); 112 (digital repository); Figure 11 (IP address, information); page 11, lines 16-22; and page 19, lines 20-24).

Further, Claim 16 recites that the collecting step comprises automatically requesting the information from the device over the first network, without receiving any instructions from the remote monitoring computer requesting that the information be collected from the device, which finds supports, e.g., in Figure 4, steps S408 and S410; and page 15, lines 5-8.

Further, Claim 16 recites that the sending step comprises automatically sending the information to the remote monitoring computer, after initialization of the local monitoring computer, without receiving any instructions from the remote monitoring computer requesting that the collected information be sent, which finds supports, e.g., in Figure 4, step S422; Figure 5, Figure 7; and page 15, lines 10-13.

Claim 25 is directed to a computer program product.

In particular, Claim 25 recites a non-carrier wave computer storage medium; and a computer program code mechanism embedded in the computer storage medium for causing a computer to remotely monitor a device connected to a first network with a remote monitoring computer connected to a second network, which finds supports, e.g., in Figure 12 and pages 20-24 of the specification.

Further Claim 25 recites that the computer program code mechanism includes a first computer code device configured to collect information from the device over the first network using an SNMP protocol, which finds supports, e.g., in Figure 1, elements 105 (local monitoring computer); 108A (device); 106 (first network). See also page 7, lines 17-21 (SNMP); and page 9, lines 6-10 (SNMP).

Further Claim 25 recites that the computer program code mechanism includes a second computer code device configured to send the collected information to the remote monitoring computer in association with an IP address of the device via a wide area network using a protocol, which finds supports, e.g., in Figure 1, elements 111 (remote monitoring computer); 114 (second network); and 110 (wide area network); and page 9, line 22 to page 10, line 7 (send to remote monitor).

Further, Claim 25 states that the first computer code device is configured to automatically request the information from the device over the first network, without receiving any instructions from the remote monitoring computer requesting that the information be collected from the device, which finds supports, e.g., in Figure 4, steps S408 and S410; and page 15, lines 5-8.

Further, Claim 25 states that, after initialization of the computer, the second computer code device is configured to automatically send the collected information to the remote monitoring computer, without receiving any instructions from the remote monitoring computer requesting that the collected information be sent, which finds supports, e.g., in Figure 4, step S422; Figure 5, Figure 7; and page 15, lines 10-13.

Claim 34 is directed to a system for remotely monitoring network devices.

In particular, Claim 34 recites a computer for collecting information from a device connected to a first network using an SNMP protocol, which finds supports, e.g., in Figure 1, elements 105 (computer); 108A (device); 106 (first network). See also page 7, lines 17-21 (SNMP); and page 9, lines 6-10 (SNMP).

Further, Claim 34 recites means for sending the information collected by the computer to a remote monitoring computer connected to a second network via a wide area network using a protocol, which finds supports, e.g., in Figure 1, elements 111 (remote

monitoring computer); 114 (second network); and 110 (wide area network). See also page 9, line 22 to page 10, line 7 (send to remote monitor).

Further, Claim 34 recites means for receiving, by the remote monitoring computer, the information sent by the means for sending, which finds supports, e.g., in Figure 8.

Further, Claim 34 recites means for storing the information received by the means for receiving in association with an IP address of the device in a digital repository connected to the second network, which finds supports, e.g., in Figure 9 and Figure 1, element 111 (remote monitoring computer); 112 (digital repository); Figure 11 (IP address, information); page 11, lines 16-22; and page 19, lines 20-24).

Further, Claim 34 recites that the computer comprises means for automatically requesting the information from the device over the first network, without receiving any instructions from the remote monitoring computer requesting that the information be collected from the device, which finds supports, e.g., in Figure 4, steps S408 and S410; and page 15, lines 5-8.

Further, Claim 34 recites that, after initialization of the computer, the means for sending comprises means for automatically sending the information to the remote monitoring computer, without receiving any instructions from the remote monitoring computer requesting that the collected information be sent, which finds supports, e.g., in Figure 4, step S422; Figure 5, Figure 7; and page 15, lines 10-13.

## VI. GROUND OF REJECTION TO BE REVIEWED ON APPEAL

The ground of rejection being appealed is as follows:

whether the teachings of U.S. Patent No. 6,108,782 to Fletcher et al. (hereinafter "the '782 patent") anticipates the subject matter of each of Claims 1-12, 14-19, 21-28, 30, and 32-35 under U.S.C. § 102(e);

## VII. ARGUMENT

### Claims 1-12, 14-19, 21-28, 30, and 32-35

Claim 1 is directed to a computer implemented remote device monitoring system, comprising: (1) a local monitoring computer configured to collect information from a device connected to a first network using an SNMP protocol, and to send the information to a remote monitoring computer connected to a second network via a wide area network using a protocol; and (2) the remote monitoring computer configured to receive the information using the protocol and to store the information in association with an IP address of the device in a digital repository connected to the second network. Further, Claim 1 clarifies that the local monitoring computer is configured to automatically request the information from the device over the first network, without receiving any instructions from the remote monitoring computer requesting that the information be collected from the device. Further, Claim 1 clarifies that, after initialization of the local monitoring computer, the local monitoring computer is configured to automatically send the information to the remote monitoring computer, without receiving any instructions from the remote monitoring computer requesting that the collected information be sent.

Regarding the rejection of Claim 1, the '782 patent is directed to a method for the distributed collection of network statistics, including the steps of gathering network statistics at a plurality of nodes distributed in a network; transmitting data containing the statistics to a collector; combining the statistics from the plurality of nodes into group network statistics; and reporting the network performance data based on the compiled statistics from the collector to a network manager, wherein the multiple nodes respond to a multicast poll from the collector, but that flooding of the collector is prevented by having each node delay its response by a random value. As shown in Figure 1, the '782 patent discloses a plurality of

distributed remote network monitor (dRMON) agents that are software or software plus hardware components placed within a corresponding plurality of end stations (ESs). Further, the '782 patent discloses that, based on a polling packet from the collector (see elements 60, 61a, 61b, and 62 in Figure 1), the dRMON agents forward their statistics and/or capture packets to the dRMON collector, which exists somewhere in the network. Further, the '782 patent discloses that the dRMON agents are implemented in the C programming language and consist of executable code that is launched each time an end station is started or rebooted, and that the end station user is unaware of the agent's presence and can do nothing with regard to reconfiguring the end station.<sup>1</sup> Further, regarding the capturing of packets from the end station, the '782 patent discloses that "an NDIS Desktop Agent type module (DTA) is used to bind to the network adapter driver, thus establishing a source of directed packets to analyze as well as a means to communication with the dRMON collector via the network. Multiple NIC binding may be supported by the agent and may allow the agent to monitor traffic on different segments having different layer 1 protocols."<sup>2</sup>

However, Applicants respectfully submit that the '782 patent fails to disclose a local monitoring computer configured to collector information from a device connected to a first network using an SNMP protocol, wherein the local monitoring computer is configured to automatically request the information from the device over the first network, as recited in Claim 1. Applicants respectfully submit that the dRMON agents disclosed by the '782 patent do not collect information from the '782 end stations over a network using the SNMP protocol. Rather, the '782 patent discloses that the dRMON agents are software applications or software/hardware devices residing on the end stations. Further, the '782 patent does not disclose that SNMP is used by the agents to collect information from the devices. The section in the '782 patent cited by the outstanding Office Action regarding SNMP (column 9,

---

<sup>1</sup> See '782 patent, column 8, lines 29-36.

<sup>2</sup> '782 patent, column 8, lines 37-45.



lines 39 and 40) states only that the collector can make information available to management applications using either SNMP or a web browser. However, this section says nothing about how the agents collect information from the end stations. Moreover, as discussed above, the '782 patent discloses that the agents "monitor" the network adapter driver to capture packets. Thus, Applicants respectfully submit that the dRMON agents disclosed by the '782 patent do not collect information from a device connected to a first network using an SNMP protocol over the first network, as required by Claim 1. To the contrary, the '782 agents are software applications (and/or hardware included on the end station) that are used to directly monitor and capture packets from the end station.

Further, Applicants respectfully submit that the '782 patent fails to disclose that the local monitoring computer is configured to automatically send the information to the remote monitoring computer, without receiving any instructions from the remote monitoring computer requesting that the collected information be sent. Regarding communication between the dRMON agents and the dRMON collector, the '782 patent discloses that several steps are taken "...to help optimize and minimize network traffic between the collector and the agent."<sup>3</sup> The '782 patent discloses that one such step to minimize communication is that "agents generate a statistics response packet only in response to a request by a collector. ***In general, there is no other traffic generated by agents unless specifically requested by the collector in a multicast packet.***"<sup>4</sup> Accordingly, Applicants respectfully submit that the '782 patent clearly does not disclose that the dRMON agents are configured to automatically send the collected information to the collector without receiving instructions from the remote monitoring computer, as would be required by Claim 1. On the contrary, the '782 patent makes clear that the collector specifically request information from the agents.

---

<sup>3</sup> '782 patent, column 13, lines 5-7.

<sup>4</sup> '782 patent, column 13, lines 27-31. Emphasis added.

In this regard, Applicants note that the Advisory Action dated August 15, 2007, states that this limitation is disclosed by the '782 patent in column 9, lines 65-66. That passage in the '782 patent is directed to a block diagram of a dRMON collector, and states that like the agent, "the Collector loads automatically when the system starts..."<sup>5</sup> While Applicants agree that this passage makes use of the word "automatically," which is also recited in Claim 1, the passage merely states that the collector software loads automatically when the system starts. However, Applicants respectfully submit that this has nothing to do with the local monitoring computer being configured to automatically send the information to the remote monitoring computer, without receiving any instructions from the remote monitoring computer requesting that the collected information be sent, as recited in Claim 1.

For the reasons stated above, Applicants respectfully traverse the rejection of Claim 1 (and all associated dependent claims) as anticipated by the '782 patent.

Since the '782 patent does not disclose the functions of the local monitoring computer recited in Claim 1, it can not disclose the sending step recited in Claim 16, the second computer code recited in Claim 25, and the means for sending recited in Claim 34. Accordingly, for reasons analogous to the reasons stated above for the patentability of Claim 1, Applicants respectfully traverse the rejections of Claims 16, 25, and 34 (and all associated dependent claims) as anticipated by the '782 patent.

---

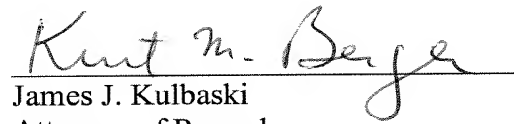
<sup>5</sup> '782, column 9, lines 65-66.

VIII. CONCLUSION

For the foregoing reasons, Applicant respectfully submits that each of Claims 1-12, 14-19, 21-28, 30, and 32-35 patentably defines over the teachings of the '782 patent. Therefore, the outstanding rejections must be REVERSED.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.



James J. Kulbaski  
Attorney of Record  
Registration No. 34,648

Customer Number  
**22850**

Kurt M. Berger, Ph.D.  
Registration No. 51,461

Tel: (703) 413-3000  
Fax: (703) 413 -2220  
(OSMMN 08/03)  
JJK/KMB:smi

I:\ATTY\KMB\198's\198775US\198775US.APPEAL.BRIEF.DOC

CLAIMS APPENDIX

1. (Rejected) A computer-implemented remote device monitoring system, comprising:

a local monitoring computer configured (1) to collect information from a device connected to a first network using an SNMP protocol, and (2) to send the information to a remote monitoring computer connected to a second network via a wide area network using a protocol; and

the remote monitoring computer configured to receive the information using the protocol and to store the information in association with an IP address of the device in a digital repository connected to the second network,

wherein the local monitoring computer is configured to automatically request the information from the device over the first network, without receiving any instructions from the remote monitoring computer requesting that the information be collected from the device; and

wherein, after initialization of the local monitoring computer, the local monitoring computer is configured to automatically send the information to the remote monitoring computer, without receiving any instructions from the remote monitoring computer requesting that the collected information be sent.

2. (Rejected) The system of claim 1, wherein the information comprises at least one of status information corresponding to the device and configuration information corresponding to the device.

3. (Rejected) The system of claim 2, wherein the device comprises a printer.

4. (Rejected) The system of claim 2, wherein the status information comprises at least one of a low paper indicator, a no paper indicator, a low toner indicator, a no toner indicator, a door open indicator, a jammed indicator, an offline indicator, and a service-requested indicator.

5. (Rejected) The system of claim 2, wherein the configuration information comprises at least one of a manufacturer of the device, a model of the device, a serial number of the device, a media access control address, an Internet protocol address, a company name, a street address, a city, a state, a postal code, a physical location of the device, a contact person for the device, a phone number for the contact person, and an e-mail address for the contact person.

6. (Rejected) The system of claim 1, wherein at least a portion of the wide area network comprises the Internet.

7. (Rejected) The system of claim 1, wherein the protocol comprises at least one of a simple mail transfer protocol and an Internet mail access protocol.

8. (Rejected) The system of claim 1, wherein at least a portion of at least one of the first network and the second network comprises an intranet.

9. (Rejected) The system of claim 1, wherein the digital repository comprises a database.

10. (Rejected) The system of claim 1, wherein the local monitoring computer is further configured to store the collected information in a first digital repository connected to the first network, and to retrieve the information from the first digital repository.

11. (Rejected) The system of claim 10, wherein the digital repository comprises a database.

12. (Rejected) The system of claim 1, wherein the local monitoring computer comprises a computer readable medium encoded with processor readable instructions that comprise at least one of a dynamic link library, a static link library, a script, a JAVA class, a C++ class, and a C library routine.

13. (Canceled).

14. (Rejected) The system of claim 1, wherein the remote monitoring computer is further configured to store the information in the digital repository through an open database connectivity interface.

15. (Rejected) The system of claim 10, wherein the local monitoring computer is further configured to store the information in the first digital repository through an open database connectivity interface.

16. (Rejected) A method for remotely monitoring network devices, comprising:  
collecting, by a local monitoring computer, information from a device connected to a first network using an SNMP protocol;

sending, by the local monitoring computer, the information collected in the collecting step to a remote monitoring computer connected to a second network via a wide area network using a protocol;

receiving, by the remote monitoring computer, the information sent in the sending step; and

storing the information received in the receiving step in association with an IP address of the device in a digital repository connected to the second network,

wherein the collecting step comprises automatically requesting the information from the device over the first network, without receiving any instructions from the remote monitoring computer requesting that the information be collected from the device; and

wherein the sending step comprises automatically sending the information to the remote monitoring computer, after initialization of the local monitoring computer, without receiving any instructions from the remote monitoring computer requesting that the collected information be sent.

17. (Rejected) The method of claim 16, wherein the information comprises at least one of status information corresponding to the device and configuration information corresponding to the device.

18. (Rejected) The method of claim 16, wherein the device comprises a printer.

19. (Rejected) The method of claim 16, wherein at least a portion of the wide area network comprises the Internet.

20. (Canceled).

21. (Rejected) The method of claim 16, wherein the protocol comprises at least one of a simple mail transfer protocol and an Internet access protocol.

22. (Rejected) The method of claim 16, wherein the digital repository comprises a database.

23. (Rejected) The method of claim 16, further comprising:  
storing the collected information collected in the collecting step in a first digital repository; and  
retrieving the information stored in the step of storing the collected information from the first digital repository.

24. (Rejected) The method of claim 23, wherein the first digital repository comprises a database.

25. (Rejected) A computer program product, comprising:  
a non-carrier wave computer storage medium; and  
a computer program code mechanism embedded in the computer storage medium for causing a computer to remotely monitor a device connected to a first network with a ~~monitor~~ remote monitoring computer connected to a second network, the computer program code mechanism comprising:

a first computer code device configured to collect information from the device over the first network using an SNMP protocol, and



a second computer code device configured to send the collected information to the remote monitoring computer in association with an IP address of the device via a wide area network using a protocol, wherein the first computer code device is configured to automatically request the information from the device over the first network, without receiving any instructions from the remote monitoring computer requesting that the information be collected from the device;

wherein, after initialization of the computer, the second computer code device is configured to automatically send the collected information to the remote monitoring computer, without receiving any instructions from the remote monitoring computer requesting that the collected information be sent.

26. (Rejected) The computer program product of claim 25, wherein the information comprises at least one of status information corresponding to the device and configuration information corresponding to the device.

27. (Rejected) The computer program product of claim 25, wherein the device comprises a printer.

28. (Rejected) The computer program product of claim 25, wherein at least a portion of the wide area network comprises the Internet.

29. (Canceled).

30. (Rejected) The computer program product of claim 25, wherein the protocol comprises at least one of a simple mail transfer protocol and an Internet access protocol.

31. (Canceled)

32. (Rejected) The computer program product of claim 25, wherein the computer program code mechanism further comprises:

a third computer code device configured to store the information collected by the first computer code device in a first digital repository; and

a fourth computer code device configured to retrieve the information from the first digital repository.

33. (Rejected) The computer program product of claim 32, wherein the first digital repository comprises a database.

34. (Rejected) A system for remotely monitoring network devices, comprising:

a computer for collecting information from a device connected to a first network using an SNMP protocol;

means for sending the information collected by the computer to a remote monitoring computer connected to a second network via a wide area network using a protocol;

means for receiving, by the remote monitoring computer, the information sent by the means for sending; and

means for storing the information received by the means for receiving in association with an IP address of the device in a digital repository connected to the second network,

wherein the computer comprises means for automatically requesting the information from the device over the first network, without receiving any instructions from the remote monitoring computer requesting that the information be collected from the device; and

wherein, after initialization of the computer, the means for sending comprises means for automatically sending the information to the remote monitoring computer, without receiving any instructions from the remote monitoring computer requesting that the collected information be sent.

35. (Rejected) The system of claim 34, wherein:

the protocol is at least one of a simple mail transfer protocol and an Internet mail access protocol.

EVIDENCE APPENDIX

None

RELATED PROCEEDING APPENDIX

None